¿Estáis preparados?

Solución del Reto 4: ingeniería social

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL

Índice

R.4 Solución al RETO 4: ataque por ingeniería social

Este es el material que se ha de entregar al equipo cuando hayan debatido sobre el incidente.

1.1 ¿Qué puedes hacer?

- Llamar al banco para que anule los movimientos fraudulentos.
- Poneros en contacto con la policía y con Incibe para denunciar los hechos.
- Crear credenciales personales para cada una de las personas autorizadas a manejar la cuenta de facturación. Dar permisos sobre la cuenta de facturación y sobre otros servicios críticos sólo a los empleados que realmente van a realizar esta labor, con credenciales de acceso personalizadas.
- Adoptar una política de seguridad. Con medidas como las de utilizar contraseñas robustas, no transmitirlas por correo electrónico, etc.
- Lanzar unas sesiones de formación periódicas para detectar ataques de ingeniería social.

R.4 Ingeniería Social

1.2 ¿Qué no debes hacer?

- Ocultar el problema.
- Intentar resolverlo tú sólo, sin buscar ayuda.
- Buscar culpables antes de analizarlo todo.
- Dar permisos a los servicios críticos de la empresa (como la cuenta de facturación), de manera indiscriminada, a todos los usuarios.
- Cuando hay algo sospechoso o cometo algún error, lo oculto para que no se note y no me echen las culpas.
- Echarle la culpa a otro a ver si cuela.

1.3 Lecciones aprendidas: ¿cómo podrías evitarlo?

- Formar y sensibilizar a todo el personal sobre cómo actuar ante este tipo de incidentes. Hemos planificado sesiones de concienciación para identificar este tipo de correos y no dejarnos engañar.
- Estar preparado por si ocurre un incidente, es decir tener un procedimiento de gestión de incidencias que todo el mundo conozca para saber cómo actuar.
- Tener a mano la lista de contactos de apoyo y de denuncia para estos casos.
- Analizar nuestros riesgos pues está claro que esto puede ocurrir pero no debe volver a pasar. Tomar medidas: revisar los procedimientos de contraseñas y correo electrónico.

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL